36C10B18Q3124 0001

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO.	1. CONTRACT ID CODE	PAGE	OF PAGES
		1	71

2. AMENDMENT/MODIFICATION NUMBER	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NUMBER	5. PROJECT NUMBER (if applicable)
0001			TAC-18-49850

6. ISSUED BY	CODE	7. ADMINISTERED BY (If other than Item 6)	CODE
Department of Veterans Affairs Technology Acquisition Center 23 Christopher Way Eatontown NJ 07724		Department of Veterans Affairs Technology Acquisition Center 23 Christopher Way Eatontown NJ 07724	

8. NAME AND ADDRESS OF CONTRACTOR (Number, street, county, State and ZIP Code)	(X)	9A. AMENDMENT OF SOLICITATION NUMBER
To all Offerors/Bidders		36C10B18Q3124
	X	9B. DATED (SEE ITEM 11)
		10A. MODIFICATION OF CONTRACT/ORDER NUMBER
		10B. DATED (SEE ITEM 13)
CODE / FACILITY CODE		

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☒ is extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	
	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor ☐ is not, ☐ is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

See continuation page

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
15B. CONTRACTOR/OFFEROR _____ (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA BY _____ (Signature of Contracting Officer)	16C. DATE SIGNED

CONTINUATION PAGE:

The purpose of this Amendment A0001, to Request for Quote (RFQ) 36C10B18Q3124 titled "VA API Development and Operations," is as detailed below. All changes to RFQ 36C10B18Q3124 have been captured in track changes.

1. Performance Work Statement (PWS) Paragraphs 3.0 Scope of Work and 5.3 VA API Gateway Development and Operations – Optional Task (Labor Hour) are hereby revised to clarify the use of alternative API Gateway products.

2. PWS Paragraph 5.1.3, Key Personnel: The statement for "The Contractor shall identify statement of qualification for individuals that will fulfill the key personnel positions identified below" is hereby deleted.

3. PWS Paragraph 5.2.1 API Development is hereby revised to clarify the VA Product team and the Contractor sprint team shall determine the acceptance criteria for the sprint and populate the Sprint Backlog in the sprint planning meeting.

2. Section E.10, Quote Submission Requirements, has been revised to clarify the three sections as (i) Technical; (ii) Price Factors; and (iii) Solicitation, Quote, and Award Documents and certifications/representations.

5. The Quote Due Date is hereby extended to September 10, 2018 at 12:00PM EST.

Except as provided herein, all other terms and conditions of RFQ 36C10B18Q3124 remain unchanged and in full force and effect.

B.5 PERFORMANCE WORK STATEMENT

PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS (VA)
Office of Information & Technology
Enterprise Program Management Office (EPMO)

VA API Development and Operations

Date: August 32~~0~~, 2018
TAC-18-49850
Version Number: 1.1~~0~~

1.0 BACKGROUND

The Department of Veterans Affairs (VA) requires Contractor support to design, develop, and maintain various aspects of the VA Application Programming Interface (API) platform, including but not limited to platform design, API development and maintenance, developer documentation, and product management best practices to work with teams internal and external to VA, using modern software development methods and tools.

From shopping for car insurance, to paying bills online, to scheduling a dentist appointment, Americans expect the places where they do business to offer easy-to-use, secure digital tools. Veterans, caregivers, Servicemembers, Veterans Service Organizations (VSO), and VA's other users are no different; they expect VA to offer a digital experience on par with the private sector companies they interact with in their day-to-day lives.

VA is taking an API-first strategy to deliver the high quality digital experiences our users expect. A single set of APIs will power every VA digital service, and these same APIs will be exposed to approved third parties to build products and applications on top of VA services and data. These APIs across every vertical of VA's business will enable VA users to receive a consistent, high quality experience across all VA communication channels (e.g., digital, phone, mail, in-person, etc.).

The health industry is quickly converging on the Fast Healthcare Interoperability Resources (FHIR) standard to enable enhanced data interoperability between both internal and external systems. API-enabled and FHIR based solutions are easier for developers to implement as it makes use of modern web standards and RESTful architectures with more easily understood specifications. By liberating data and enhancing interoperability with FHIR, VA will shift data ownership to Veterans, making it more readily available.

In the benefits space, VSOs and other third parties spend significant amounts of time manually looking in VA systems to check on the status of a claim for a Veteran they are working with, or to find out if a rating has been granted. If VA were instead able to provide APIs to this information, authorized individuals and organizations would be able to access it more readily, improving the experience they can provide for Veterans and reducing VA costs.

Finally, one of VA's core competencies should be "knowing and sharing what we know" about a Veteran, including data such as service history, accurate mailing address, and disability ratings. VA should be able to share this information with Veterans and Veteran-authorized third parties. Veterans should not need to upload a Department of Defense Form 214 (DD214) to a website to prove their military service history or discharge status, which is not only difficult for some Veterans but also presents identity theft risks by needlessly sharing personally identifiable information (PII). With APIs, VA plans to put this data back in the hands of Veterans so that they can use it more efficiently and securely, resulting in a better, more personalized digital experience for Veterans.

This contract is not for creating a specific number of APIs, or APIs in a single domain, but rather for agile, cross-functional teams that can work alongside a VA product team to prioritize, build, operate, and iterate on APIs across many parts of VA. It will include creating new APIs, refactoring or replatforming existing APIs, building on top of existing APIs, and/or working with other teams to improve their APIs and/or expose their data in a modern way.

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the following:

1. "Federal Information Security Modernization Act of 2014"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems, March 2016
4. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
5. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
6. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters
7. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
8. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016
9. Office of Management and Budget (OMB) Circular A-130, "Managing Federal Information as a Strategic Resource," July 28, 2016
10. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
11. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
12. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015
13. VA Handbook 6500.1, "Electronic Media Sanitization," November 03, 2008
14. VA Handbook 6500.2, "Management of Breaches Involving Sensitive Personal Information (SPI)", July 28, 2016
15. VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of VA Information Systems," February 3, 2014
16. VA Handbook 6500.5, "Incorporating Security and Privacy in System Development Lifecycle", March 22, 2010
17. VA Handbook 6500.6, "Contract Security," March 12, 2010
18. VA Handbook 6500.8, "Information System Contingency Planning", April 6, 2011
19. One-VA Technical Reference Model (TRM) (reference at https://www.va.gov/trm/TRMHomePage.aspx)
20. VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 15, 2014
21. VA Handbook 6508.1, "Procedures for Privacy Threshold Analysis and Privacy Impact Assessment," July 30, 2015
22. VA Handbook 6510, "VA Identity and Access Management", January 15, 2016
23. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
24. NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, June 10, 2014
25. NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, January 22, 2015
26. OMB Memorandum, "Transition to IPv6", September 28, 2010
27. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015

28. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
29. NIST SP 800-63-3, 800-63A, 800-63B, 800-63C, Digital Identity Guidelines, June 2017
30. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
31. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access", January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
32. "Veteran Focused Integration Process (VIP) Guide 2.0", May 2017, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371
33. VA Memorandum "Use of Personal Email (VAIQ #7581492)", April 24, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
34. VA Memorandum "Updated VA Information Security Rules of Behavior (VAIQ #7823189)", September, 15, 2017, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
35. API Best Practices
    a. 18 F API Standards (https://github.com/18F/api-standards)
    b. WH API Standards https://github.com/WhiteHouse/api-standards
36. Building Twelve-Factor App (https://12factor.net/).
37. Experience with incorporating and using open source technologies (https://sourcecode.cio.gov/OSS/).
38. The Agile Manifesto (http://www.agilemanifesto.org/)
39. The U.S. Digital Services Playbook (https://playbook.cio.gov/)
40. The Techfar Hub (https://techfarhub.cio.gov/)
41. VA Enterprise Cloud (VAEC) Technical Reference Guide for Acquisition Support, October 2017 (Attachment 001)

3.0 SCOPE OF WORK

The Contractor shall provide VA with agile development and operations of APIs and support for the VA API Gateway. This includes project management, product management, requirements refinement, human centered design, iterative development, user research and usability testing, standards enforcement, automated testing, performance metrics definition and reporting, automated monitoring and performance reporting, and continuous integration / continuous delivery (CI/CD) for the development and enhancement of APIs and the API Gateway. Through the Government's prioritization of the backlog, the Contractor shall prioritize execution of all aspects of the API Gateway. The Contractor shall also work to ensure that all APIs are deployed or migrated into a VA designated cloud.

The Government will provide the Contractor with access to the VAEC to include the credits required for all VAEC cloud development, testing, and production environment requirements. The VAEC includes a secure dedicated Wide Area Network connection between VA and the VAEC Cloud Service Provider (CSP). The Contractor shall not be responsible for buying cloud credits for this contract. The VAEC is currently supported by two Federal Risk and Authorization Management Program (FedRAMP) High Certified and VA ATO approved CSPs. Both VAEC environments provide access to all of each CSP's FedRAMP Authorized Services in their respective cloud to implement the proposed solution. In addition, each VAEC CSP provides

a set of common shared services such as security scanning; Active Directory and single-sign (SSO); PIV integration; and performance monitoring to facilitate solution implementation. Specifications for each VAEC CSP, including access requirements, will be provided at the project kick off meeting.

A Minimum Viable Product (MVP) API Gateway has already been stood up in AWS but the contractor may propose the use of a different VAEC cloud if they can demonstrate how the alternative will provide equal to or superior performance than AWS at equal to or lower cost to the Government, including transition costs. The MVP API Gateway is using open-source Kong, but the Contractor may propose the use of other API Gateway products if they can demonstrate how the product and platform will provide equal to or superior performance than Kong and adequately present to the Government the value of utilizing the alternative products. ~~at equal to or lower cost to the Government, including transition costs~~.

The Contractor's support and solutions shall align with the U.S. Digital Services Playbook (https://playbook.cio.gov). The Contractor shall be familiar with the concepts in each play and implement them in its approaches and support.

4.0 PERFORMANCE DETAILS

This is a hybrid Firm-Fixed Price (FFP)/Time-and-Materials (T&M)/Labor-Hour type contract.

4.1 PERFORMANCE PERIOD

The Period of Performance shall consist of one 12-month period.

There are 10 Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

The other six are set by a day of the week and month:

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.2 PLACE OF PERFORMANCE

Tasks under this PWS may be performed at Contractor facilities. The Contractor is expected to attend in-person VA meetings and / or working sessions as requested by VA.

4.3 TRAVEL

The Government anticipates travel under this effort to perform the tasks associated with the effort, as well as to attend program-related meetings or conferences throughout the PoP. The meeting locations shall be located in Washington, DC. The Contractor shall include all estimated travel costs in its FFP line items. These costs will not be directly reimbursed by the Government. The following is the estimated travel for the FFP portion of the effort.

Purpose	Number of Trips	Number of Days	Number of Staff
Kick-off Meeting	1	1-3	4
Quarterly Program Reviews	4	1-3	4

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 REPORTING REQUIREMENTS

The Contractor shall deliver Monthly Status Reports. These reports shall provide accurate, timely, and complete project information supporting reporting Requirements. The Monthly Status Report shall include the following data elements and reporting capability shall address the below requirements:

a. Project Name
b. Overview and description of the contract
c. Overall high-level assessment of contract progress
d. All work in-progress and completed during the reporting period
e. Identification of any contract related issues uncovered during the reporting period and especially highlight those areas with a high probability of impacting schedule, cost or performance goals and their likely impact on schedule, cost, or performance goals
f. Explanations for any unresolved issues, including possible solutions and any actions required of the Government and/or Contractor to resolve or mitigate any identified issue, including a plan and timeframe for resolution
g. Status on previously identified issues, actions taken to mitigate the situation and/or progress made in rectifying the situation.
h. Work planned for the subsequent two reporting periods, when applicable
i. Provide expenditures based upon your proposed spend plan.
j. Workforce staffing data showing all Contractor personnel performing on the effort by task during the current reporting period along with status of their background investigation/VA clearance and biographies. After the initial labor baseline is provided, each Monthly Status Report shall identify any changes in staffing identifying each person who was added to the contract or removed from the contract.
k. Original schedule of deliverables at the start of each sprint and the corresponding deliverables made during the current reporting period.
l. Cost analysis that includes consumption of cloud resources by API.
m. Software licenses at or nearing end of life and software security certificates nearing expiration.

The Contractor shall communicate with VA so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

For each T&M/Labor-Hour task, indicate:

a. Summary of work performed
b. Expenditures for the reporting period, to include prime labor and each subcontractor identified separately
c. Contract Line Item Number expenditure
d. Burn rate
e. Percentage of work completed

Deliverable:

A. Monthly Status Report

5.1.2 TECHNICAL KICK-OFF MEETING

The Contractor shall conduct a kick-off meeting with the VA PM, Contracting Officer's Representative (COR) and the Contracting Officer (CO). The meeting shall be held within 10 business days after contract award. The kick-off meeting shall be an in-person meeting in a VA or VA-approved Contractor facility. The Contractor shall propose an agenda for VA COR approval three days prior to the meeting. The Contractor shall provide meeting minutes capturing discussion, agreements, and action items resulting from the kick-off meeting. The kick-off meeting shall address post award topics and shall present the Contractor's draft plans and approach for meeting PWS requirements.

5.1.3 KEY PERSONNEL

Specific expertise and experience in product management, engineering, and operating highly available products is essential for accomplishing the tasks outlined in this PWS. ~~The Contractor shall identify statements of qualifications for individuals that will fulfill the key personnel positions identified below.~~

Key Roles:

- Product Manager:
  - Experience managing entire agile software development lifecycle for a project of at least one million dollars up to and including production delivery and some phase of post-delivery support.
  - Experience as a product manager accountable for delivery with at least 10 software professionals with a duration of greater than one year.
  - Demonstrated success with delivering digital products.
- Chief Engineer:
  - Background as a Software Engineer for at least five years, including experience as a Software Engineer for at least one project in one of the VAEC's CSP Vendors Clouds.
  - Chief Architect or Senior Engineer on a production system in one of the VAEC CSP Vendors Clouds.
  - Demonstrated knowledge and use of modern software development and Dev/Ops tools, including GitHub.
- Chief Operations Manager:
  - Background as a Software Engineer, Site Reliability Engineer, or DevOps Engineer for at least three years.
  - Experience running a 24x7 Software based System for at least 6 months.

- Experience with oversight of an operations team of at least 5 people for at least one year.
- Experience in Incident Management for a software based system.
- Experience with oversight of a team running a trouble ticket system.
- Demonstrated success using modern DevOps methods and tools including automated testing tools and monitoring tools.
- Demonstrated ability to drive frequent release cycles (daily / weekly)

Any personnel the Contractor offers as substitutes shall have the ability and qualifications equal to or better than the key personnel which are being replaced. If any change to a key personnel position becomes necessary, the Contractor shall immediately notify the VA PM and COR in writing, but whenever possible Contractor shall notify the VA PM of substitutions in personnel in writing 30 calendar days prior to making any change in key personnel, and provide a detailed explanation of the circumstances necessitating the proposed substitution and shall demonstrate that the proposed replacement personnel are of at least substantially equal ability and qualifications as the individual originally proposed for that position.

The Contractor agrees that it has a contractual obligation to mitigate the consequences of the loss of Key Personnel and shall promptly secure any necessary replacements in accordance with (IAW) this PWS section. Failure to replace a Key Person pursuant to this clause and without a break in performance of the labor category at issue shall be considered a condition endangering contract performance and may provide grounds for termination for cause.

5.1.4 PRIVACY AND HIPAA TRAINING

The Contractor shall submit status of VA Privacy and Information Security Awareness training for all individuals engaged on the task. The status reporting shall identify; a single Contractor Security Point of Contract, the names of all personnel engaged on the task, their initial training date for VA Privacy and Information Security training, and their next required training date. This information shall be submitted as part of the Weekly/ Progress Status Report.

The Contractor shall submit Talent Management System (TMS) training certificates of completion for VA Privacy and Information Security Awareness training. The Contractor shall also provide VA Privacy and Information Security Awareness Signed Rules of Behavior, and VA Health Insurance Portability and Accountability Act (HIPAA) Certificate of Completion IAW Section 9, Training, from Appendix C of the VA Handbook 6500.6, "Contract Security".

Deliverables:

A. TMS Training Certificates of Completion for VA Privacy and Information Security Awareness Training
B. VA Privacy and Information Security Awareness Signed Rules of Behavior
C. VA HIPAA Certificate of Completion

5.2 VA API Development & Operations

VA is taking an API-first strategy to deliver the high quality digital experiences our users expect. A single set of APIs will power every VA digital service, and these same APIs will be exposed to approved third parties to build products and applications on top of VA services and data. These APIs across every vertical of VA's business will enable VA users to receive a consistent, high quality experience across all VA communication channels (e.g., digital, phone, mail, in-person, etc.).

5.2.1 API Development

The Contractor shall provide cross-functional Contractor Sprint Teams for the development of VA APIs. This contract is not for creating a specific number of APIs, or APIs in a single domain, but rather for agile, cross-functional teams that can work alongside a VA product team to prioritize, build, operate, and iterate on APIs across many parts of VA. It will include creating new APIs, refactoring or replatforming existing APIs, building on top of existing APIs, and/or working with other teams to improve their APIs and/or expose their data in a modern way. The specific scope of functionality of the tasks will be determined by VA API Product Owners and the VA PM/COR, prior to sprint commencing. At the beginning of each two-week sprint, each Contractor Sprint Team shall initiate, coordinate, and participate in a Sprint Planning Meeting and develop a Sprint Plan with the VA Project Team, including the VA PM, COR, designated VA Product Owner and additional stakeholders, to plan the work to be accomplished for the sprint. Additionally, the VA Product team and the Contractor Sprint team shall determine the acceptance criteria for the sprint and populate the Sprint Backlog in the sprint planning meeting.

The Contractor, in collaboration with the VA Project Team, shall prioritize a backlog, estimate the relative complexity of each task, and determine the amount of work that can be accomplished in a two-week sprint. All activity scheduled in each sprint and backlog shall be captured and have status showing all work items, changes, and impediments. The Contractor shall update the Sprint Plan at the conclusion of the sprint planning. Once the Sprint Plan is accepted by the VA PM/COR and the VA Product Team, the sprint backlog may change throughout the duration of the sprint, however, the effort of work will remain constant.

The Contractor shall provide a Sprint Demonstration that confirms all functionality developed in the sprint is operational. At the Sprint Demonstration, the Contractor Sprint Team shall submit a Sprint Certification Package to the VA PM/COR for review and approval.

The Sprint Certification Package shall include a summary of the planned, accomplished, and unaccomplished work for the two-week sprint to include issues encountered and corrective actions taken as well as all artifacts produced, including any and all code (submitted to a VA source code repository, such as GitHub), during the sprint. This package, certification that all work is completed, and a demonstration that all work planned for the sprint has been fully implemented, are necessary for sprint acceptance by the Government. The Contractor shall complete all work planned for each sprint and receive VA PM/COR approval of the Sprint Certification Package for the prior sprint before beginning a new sprint.

Specifically, the Contractor shall support the building and maintaining of APIs as products, including:

a. Discovery - Conduct discovery activities on existing VA APIs as well as internal and external business process flows and functions. Work closely with VA customers to understand their needs and how those map to VA capabilities. Collect available data, user feedback, and VA stakeholder feedback and capture in a Discovery Report.
b. Product Roadmap - A comprehensive list of the APIs and API functionality that needs to be built or updated and prioritization of these based on Discovery that has happened.
c. Coordination - Participate in VA stakeholder meetings, some of which will be in-person at VA facilities, to plan building and integrating the services and change management activities including but not limited to managing agendas, minutes, action items, and collaboration tool management meetings.

d. Mock API development – Mock proposed APIs to receive feedback from potential consumers and iterate on designs quickly prior to beginning software development.
e. Code Development - Define, author, and deliver code in a way that meets private sector best practices, meets the needs of the users, and conforms to the requirements and architecture provided by the government; ensure peer reviews for code quality; incorporate testing into code development, including security scans. The Contractor shall follow an agile methodology that may result in several production releases in each sprint. The Contractor shall adhere to objectives defined in the U.S. Digital Services Playbook, as well as VA's VIP policy. All Contractor team members shall be proficient on VA tools, including GitHub, and all code should be developed in the open.
f. Integration Support – Integrate with external systems and other VA systems as needed to access appropriate data, including configuring, testing, and documenting the integration.
g. Data Migration – Develop, implement, and document any necessary data migration strategies/plan(s).
h. Deployment Activities - Plan for, create and validate the implementation and deployment instructions for use during service deployment. All deployment steps should be instrumented as infrastructure as code.
i. DevOps – Work collaboratively and cross functionally with other contractor engineering and DevOps teams to implement CI/CD processes.
j. Metrics Reporting – Develop and communicate product metrics. Metrics may include but are not limited to how many users are using the product, transactions performed, concurrent users, and value provided to the VA and API consumers. This task includes identifying and measuring baseline metrics for comparison.
k. Communication - Participating in integrated program/project teams and/or Scrum teams to enhance communication, share lessons learned, and facilitate rapid identification and mitigation of dependencies between various functional entities. The includes communication internal and external to VA.
l. Documentation - Work with the Government to architect and document, in the API Documentation, the API design specifications, including all data elements that the services provide or read.

Rights in Computer Software:

The Contractor is required to deliver the APIs, technical data, configurations, documentation or other information, including source code, during contract performance. The Government shall receive Unlimited Rights in intellectual property first produced and delivered in the performance of this contract in accordance with FAR 52.227-14, Rights In Data-General (DEC 2007). This includes all rights to source code and any and all documentation created in support thereof. License rights in any Commercial Computer Software shall be governed by FAR 52.227-19, Commercial Computer Software

Deliverables:

A. Sprint Plan
B. Product Roadmap
C. Discovery Reports
D. API Documentation
E. Sprint Certification Package and Artifacts
F. API Code

5.2.1.1 API MARKETING, OUTREACH, AND PRODUCT MANAGEMENT

The success of VA's APIs will be determined by the value they deliver to both VA and its customers. Thus, getting API consumers using the APIs and providing those consumers with a positive experience is crucial to the success of VA's API Program.

The Contractor shall provide:

a. Communication with current and potential API consumers to understand their needs and how VA can best work with them.
b. Outreach and marketing materials to inform current and potential API consumers about what is available and the value of using VA's APIs.
c. Onboarding for new consumers, as they learn about and use VA APIs.
d. Working with internal and external customers to define and measure Key Performance Indicators (KPIs) for each stage of the API customer marketing funnel and reporting out on KPI status to internal and external audiences.
e. Measuring customer satisfaction with APIs built and determining how to maximize customer satisfaction.
f. Evangelize VA APIs internally and externally to VA

5.2.2 API OPERATIONS

The Contractor shall manage and operate the APIs they develop for the life of this contract, as well as the existing three APIs that were created for the minimum viable product. The Contractor shall maintain and operate multiple environments for its APIs including, but not limited to the following environments, stood up as part of the MVP:

- Development (will not necessarily be connected to VA internal systems)
- Staging
- Production

These environments are already set up and connected to the VA network; the Contractor shall build off these existing environments rather than starting from scratch. The Contractor shall ensure that all software associated with maintaining and operating VA APIs is delivered and tracked on VA approved version control systems, such as GitHub.

The Contractor shall ensure all API Service Level Agreements, as defined below, are met, and that the APIs function correctly.

The Contractor shall:

a. Provide 24x7 Production support for VA APIs they built and manage
b. Provide Database Administration (DBA) support to cloud-based and hosted database systems for VA APIs, as needed.
c. Provide non-production environment support during normal VA business hours (8 am – 8 pm EST).
d. Work collaboratively with VA support-related stakeholders including but not limited to VA call centers, VA Customer Relationship Management (CRM) systems, VA customer service platforms, and other VA teams as needed.
e. Monitor system, network, application, database logs, and SLA metrics via VA approved monitoring tools and provide a real-time dashboard available to all program stakeholders.
f. Write and monitor synthetic monitoring scripts for VA infrastructure, APIs, and applications.
g. Provide external systems integration support through configuring, testing, and documenting the integration.

h. Perform infrastructure, operating system, and product updates, upgrades, and patches without system downtime.
i. Document in the Monthly Status Report support metrics including but not limited to: number of issues reported, problem type identification, % resolved, time for resolution, priority, severity, etc. as requested
j. Perform postmortems of any outages occurred, including root cause analysis and steps to prevent future outages

The Contractor shall provide an SLA Monitoring Plan that defines how SLA metrics will be monitored throughout the performance of the requirements, including the automated testing tools and automated SLA testing scripts that shall be used. The Contractor shall provide the SLA Monitoring Plan to the VA PM/COR for review and approval. Upon approval, the Contractor shall implement SLA monitoring IAW the approved plan and establish an SLA Dashboard that provides real time SLA metrics data available to all program stakeholders. The Contractor shall provide a VA API SLA Report monthly which shall capture data as specified in the Deliverable Metrics/SLAs.

Deliverables:

A. SLA Monitoring Plan
B. Monthly VA API SLA Report
C. Postmortems

DELIVERABLE METRICS/SLAs:

Service Availability: All deployed services shall be available and functional to serve user requests at no less than 99.9% availability. An external entity shall be able to access and receive a successful response to all APIs deployed to this platform at all times. As available on a per API basis, sample transactions or health check endpoints that are exposed to external entities shall be evaluated to determine if the response is successful. Services that are faulted due to an external entity shall have trouble tickets logged with the responsible party, with all outage time attributable to this team until the ticket is logged with the responsible entity. An automated test, IAW the approved SLA Monitoring Plan, with an execution frequency of no more than 300 seconds, and the logged reports of execution, including timing details, of that test shall be provided in the VA API SLA Report. Any faulted services attributed to an external entity shall include a record of the trouble ticket that was issued to the responsible party. This record shall include the time that it was filed, and if resolved, the time of resolution. Any maintenance window outages due to upstream or downstream maintenance shall include a record of the notification that was distributed to VA Stakeholders, and the time which the record was distributed.

Service Reachability: Services on this platform shall be reachable by internal and external entities no less than 99.9% of the time. All required routing and proxying services are correctly functioning and forwarding traffic. Services that are faulted due to an external entity shall have trouble tickets logged with the responsible party, with all outage time attributable to this team until the ticket is logged with the responsible entity. Services that are unavailable due to upstream maintenance must have an outage notification to all VA stakeholders prior to the maintenance window for attribution to the upstream team. The Contractor shall have access to the Government's published maintenance windows times and dates upon award. An automated

test, IAW the approved SLA Monitoring Plan, and the logged reports of execution, including timing details, of that test shall be provided in the VA API SLA Report.

Development Environment Availability: The APIs shall be available in the staging environment during normal VA business hours (7 am – 9 pm EST). An external entity shall be able to log into the environment, execute build and deploy jobs in the development enclave, and observe the results of those jobs with no less than 99.0% availability. An automated test, IAW the approved SLA Monitoring Plan, and the logged reports of execution, including timing details, of that test shall be provided in the VA API Platform SLA Report.

5.2.2.1 AUTHORITY TO OPERATE

The Contractor shall develop and maintain Application/Infrastructure security documentation in support of achieving and maintaining an Authority to Operate (ATO) for the API platform, inclusive of all APIs developed within it. The current MVP APIs and API Gateway are already covered by an existing full ATO at VA, which should continue to be used and updated as needed.

The Contractor shall:

a. Comply with VA ATO process.
b. Use VA FISMA control tracking system as the security documentation repository to complete and update security controls.
c. Coordinate with the VA security office and adhere to its policies.
d. Complete all VA required training (i.e. on-boarding, security, ethics, etc.) as well as provide certificates of completion to the COR.
e. Create, as directed, a wide variety of National Institute of Standards and Technology (NIST) SP800-Series security artifacts per FISMA requirements for VA systems.
f. Enter data into the VA security documentation repository, which is currently known as RiskVision and runs on a Trusted Agent FISMA application.
g. Manually review upcoming due dates for security artifacts and work with system maintainers or appropriate representatives to ensure artifacts are updated annually.
h. Support, and develop annual attestation documentation in conjunction with the system maintainer and business owner.
i. Peer review security artifacts and provide feedback to document authors.
j. Coordinate and lead quarterly familiarization exercise for Contingency Plan and Incident Response Plan.
k. Provide security documentation reporting to PMs, Information Security officers (ISO), and others.
l. Update existing Privacy Impact Analysis (PIA), System Security Plan (SSP) documents and create new PIA documents as required in support of VA apps.
m. Update ATO package as necessary

Deliverable:

A. ATO Package Documentation

5.2.2.2 MONITORING AND ALERTING

The Contractor shall support VA requirements for monitoring VA APIs, using the VAEC supported monitoring tools and processes as they exist and evolve over time. Monitoring tools may include native CSP monitoring tools (See Attachment 001 for additional details). Additionally, the Contractor shall integrate all logs with appropriate monitoring tools such as

Grafana, Prometheus, Splunk, and/or ElasticSearch. The Contractor shall create queries to support dashboards, reporting, and proactive alert generation based on system, operations, security and business needs.

The Contractor shall:

a. Create synthetic scripts to obtain real-life metrics and statistics and create dashboards, monitoring, API reporting, and proactive alerting based on synthetic script monitoring tools utilized.
b. Utilize monitoring plugins and agents to monitor numerical metrics provided by external services, servers, or equipment to collect more in-depth metrics.
c. Use Email, Short Message Service (SMS), and other methods, such as Pagerduty, for alerting schedules, escalation policies and services that escalate system, infrastructure, or security issues to a VA API on-call engineer. The Contractor shall acknowledge all alerts and remediate all issues IAW VA requirements
d. Establish and participate in monitoring of other VA upstream partner systems.
e. Assist application development teams to identify proper reporting metrics and alerts to isolate external decencies from internal services.
f. Provide assistance to internal and external teams to resolve issues during outages affecting external systems.
g. Provide an API Response Time Monitoring Report, appended to the Monthly Status Report, that provides API response time frames at the 50th, 75th, 95th, and 99th percentiles for each API.

5.2.2.3 COST AND COMPUTE OPTIMIZATION AND REPORTING

The Contractor shall review all usage of cloud computing services provided by VA associated with this effort. Plans shall be submitted and implemented quarterly on how to best optimize the environment to reduce the costs associated with resource utilization. The Contractor shall provide a breakdown of all costs by API, environment, and utilization and shall report on utilization of each class of resource as a percentage of provisioned capacity in a Monthly Utilization Report.

The Contractor shall, as part of its VA API SLA Report, include the total infrastructure expenditure and total number of request services for Cloud Resource Optimization.

Deliverables:

A. Quarterly Resource Utilization Optimization Plan
B. Monthly Utilization Report

5.2.2.4 SECURITY OPERATIONS AND MONITORING AND MANAGEMENT

The Contractor shall provide support for security operations and monitoring of VA APIs.

The Contractor shall:

a. Assign a Security officer to manage all security related task.
b. Provide 24x7x365 on call staffing for response to alerts from Network Operations Center (NOC) and/or Security Operations Center (SOC).
c. Create 24x7x365 automated monitoring and alerting
d. Continuously monitor and report the security status of the system on a regular and ad-hoc basis.

e. Provide Remediation and documentation of findings in the security assessment reports as requirement.
f. Identify and report any incidents using existing tools and strategies IAW the VA incident handling policies (VA Handbook 6500.5)
g. Conduct regular infrastructure, network and code scanning/penetration to report any security vulnerabilities based on result reports with a recommendation and/or corrective plan of action.
h. The Contractor shall proactively prepare for and actively participate in interviews, examinations, testing and reviews from the auditing community. This supports external and internal audit activities, Office of Inspector General (IG) audits, FISMA audits, third-party audits and self-assessments. The Contractor shall also support evolving VA automated security requirements such as open controls, security compliance masonry.
i. Update security documentation.
j. Create a monthly Security Assessment Report that includes:
    - Number of Incidents
    - Number Anomalies
    - Results of Penetration test
    - System down time
    - Provide Remediation and documentation of findings in the security assessment reports as requirement.

Deliverable:

A. Monthly Security Assessment Report

5.3 VA API GATEWAY DEVELOPMENT AND OPERATIONS - OPTIONAL TASK 1 (LABOR-HOUR)

The Contractor shall develop, deploy, and maintain an API Gateway that enables developers to publish, monitor, and secure APIs across VA Enterprise. This API Gateway shall handle all the tasks involved with accepting and processing concurrent API calls, including traffic management, authorization and access control, monitoring, rate limiting, API version management, and any other features required across all VA APIs. An MVP API Gateway using open-source Kong has been stood up, but the Contractor may propose the use of other API Gateway products if they can demonstrate how the product and platform will provide equal to or superior performance than Kong and adequately present to the Government the value of utilizing the alternative products. ~~at equal to or lower cost to the Government, including transition costs~~. The Contractor shall build the API Gateway to scale based on demand, and handle API requests from any authorized consumer, internal or external to VA.

The API Gateway shall be hosted at api.va.gov and shall be the single connection point for any consumer to interact with VA's APIs. The API Gateway does not include business or orchestration logic, which are covered in section 5.2 of this PWS. The development of this gateway shall follow an agile process and best practices from the U.S. Digital Service Playbook, but may not be in specific two-week sprints, depending on the amount of work needed; this optional task is therefore Labor Hour instead of Firm Fixed Price. The Operations of this API Gateway shall comply with all requirements in 5.2.2 (including sub-tasks) above. The API Gateway shall exist within the same VAEC environments and monitoring and alerting stack set up for and used in PWS Task 5.2.2; this task is only for API Gateway specific needs or requirements.

5.4 API SUPPORT TASKS - OPTIONAL TASK 2 (LABOR-HOUR)

5.4.1 API DEVELOPER PORTAL

The Contractor shall build and/or iterate on an API Developer Portal for internal and external customers to learn about the VA API platform functionality and processes and be able to use the API in a self-service capacity. This portal shall expose documentation from individual APIs to consumers in a consistent, easily understandable and usable experience, and provide information about how to use VA's APIs from both a technical and policy perspective. An MVP developer portal has been stood up and is accessible at https://developer.va.gov. The Contractor shall utilize an agile development process including creation of a backlog of features and capabilities to be presented to the VA PM and COR for review and approval prior to development commencing.

5.4.2 GOVERNANCE AND TECHNICAL SUPPORT

The Contractor shall provide support, as needed, to ensure VA has the necessary API governance in place to create a world-class API program. As defined by the VA Product Owner, this could include documenting API best practices or API standards.

Technical guidance to the product owner and development teams building other APIs and applications on top of the VA API Gateway. Defining architectural changes as needed across VA based on industry best practices and working with VA teams to implement needed changes.

5.4.3 SOFTWARE LICENSE MANAGEMENT - OPTIONAL TASK 3 (T&M)

The Contractor is responsible for procuring, managing, migrating, modifying, and terminating VA API Gateway software licenses as required. The Contractor shall coordinate with other contractors and vendors as necessary to support the procurement, management, migration, modification and termination of the software licenses. Any licenses procured for the proposed API Gateway solution shall be licensed for the benefit of VA. The software licenses listed may change over time and may be substituted for more current versions, quantities, via modification to the contract. Some necessary software licenses may include:

a. Licenses for an API Gateway, which can be open source or commercial, as defined by the Contractor in their proposal.
b. Licenses needed for building, deploying, and operating the VA API Gateway to maintain defined SLAs (separate from what is already procured for the API Operations in 5.2.2, which is included in that price).

All software licenses procured by the Contractor on behalf of VA in support of API Gateway shall be transferred to the Government at the end of the period of performance.

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

6.1.1 ONE-VA TECHNICAL REFERENCE MODEL

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to

develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

6.1.2 FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM)

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are Personal Identity Verification (PIV) card-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/VA_EA/VAEA_TechnicalArchitecture.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/enterprise_dp.asp. The Contractor shall ensure all Contractor delivered applications and systems comply with the VA Identity, Credential, and Access Management policies and guidelines set forth in the VA Handbook 6510 and align with the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance v2.0.

The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, VA Handbook 6500 Appendix F, "VA System Security Controls", and VA IAM enterprise requirements for direct, assertion based authentication, and/or trust based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of PIV card and/or Common Access Card (CAC), as determined by the business need.

The Contractor shall ensure all Contractor delivered applications and systems conform to the specific Identity and Access Management PIV requirements set forth in the Office of Management and Budget (OMB) Memoranda M-04-04, M-05-24, M-11-11, and NIST Federal Information Processing Standard (FIPS) 201-2. OMB Memoranda M-04-04, M-05-24, and M-11-11 can be found at:
https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf,
https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf, and
https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf
respectively. Contractor delivered applications and systems shall be on the FIPS 201-2 Approved Product List (APL). If the Contractor delivered application and system is not on the APL, the Contractor shall be responsible for taking the application and system through the FIPS 201 Evaluation Program.

The Contractor shall ensure all Contractor delivered applications and systems support:

1. Automated provisioning and are able to use enterprise provisioning service.
2. Interfacing with VA's MVI to provision identity attributes, if the solution relies on VA user identities. MVI is the authoritative source for VA user identity data.
3. The VA defined unique identity (Secure Identifier [SEC ID] / Integrated Control Number [ICN]).
4. Multiple authenticators for a given identity and authenticators at every Authenticator Assurance Level (AAL) appropriate for the solution.
5. Identity proofing for each Identity Assurance Level (IAL) appropriate for the solution.

6. Federation for each Federation Assurance Level (FAL) appropriate for the solution, if applicable.
7. Two-factor authentication (2FA) through an applicable design pattern as outlined in VA Enterprise Design Patterns.
8. A Security Assertion Markup Language (SAML) implementation if the solution relies on assertion based authentication. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST SP 800-63-3 guidelines.
9. Authentication/account binding based on trusted Hypertext Transfer Protocol (HTTP) headers if the solution relies on Trust based authentication.
10. Role Based Access Control.
11. Auditing and reporting capabilities.
12. Compliance with VAIQ# 7712300 Mandate to meet PIV requirements for new and existing systems. https://www.voa.va.gov/DocumentView.aspx?DocumentID=4846

The required Assurance Levels for this specific effort are Identity Assurance Level 3, Authenticator Assurance Level 3, and Federation Assurance Level 3.

6.1.3 INTERNET PROTOCOL VERSION 6 (IPV6)

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005 (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf) and September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf). IPv6 technology, in accordance with the USGv6 Profile, NIST Special Publication (SP) 500-267 (https://www.nist.gov/programs-projects/usgv6-technical-basis-next-generation-internet), the Technical Infrastructure for USGv6 Adoption (http://www-x.antd.nist.gov/usgv6/index.html), and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices shall support native IPv6 and/or dual stack (IPv6 / IPv4) connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 and/or dual stack (IPv6/ IPv4) users and all internal infrastructure and applications shall communicate using native IPv6 and/or dual stack (IPv6/ IPv4) operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services in dual stack solutions, in addition to OMB/VA memoranda, can be found at: https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

6.1.4 TRUSTED INTERNET CONNECTION (TIC)

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf.

6.1.5 STANDARD COMPUTER CONFIGURATION

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 365 ProPlus and Windows 10. However, Office 365 ProPlus and Windows 10 are not the VA standard yet and are currently approved for limited use during their rollout, we are in-process of this rollout and making them the standard by OI&T. Upon the release approval of Office 365 ProPlus and Windows 10 individually as the VA standard, Office 365 ProPlus and Windows 10 will supersede Office 2010 and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package with switches for silent and unattended installation and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) and Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG) specific to the particular client operating system being used.

6.1.6 VETERAN FOCUSED INTEGRATION PROCESS (VIP)

The Contractor shall support VA efforts IAW the Veteran Focused Integration Process (VIP). VIP is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. The VIP Guide can be found at https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371. The VIP framework creates an environment delivering more frequent releases through a deeper application of Agile practices. In parallel with a single integrated release process, VIP will increase cross-organizational and business stakeholder engagement, provide greater visibility into projects, increase Agile adoption and institute a predictive delivery cadence. VIP is now the single authoritative process that IT projects must follow to ensure development and delivery of IT products

6.1.7 PROCESS ASSET LIBRARY (PAL)

The Contractor shall utilize PAL, the OIT-wide process management tool that assists in the execution of an IT project (including adherence to VIP standards). PAL serves as an authoritative and informative repository of searchable processes, activities or tasks, roles, artifacts, tools and applicable standards or guides to assist project teams in facilitating their VIP compliant work.

6.2 SECURITY AND PRIVACY REQUIREMENTS

It has been determined that protected health information may be disclosed or accessed and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, referenced in Section D of the contract, and shall comply with VA Directive 6066.

Contractor Responsibilities:

- The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
- The Contractor shall bear the expense of obtaining background investigations.
- Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.
- The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
- The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
  - Optional Form 306
  - Self-Certification of Continuous Service
  - VA Form 0710
  - Completed Security and Investigations Center (SIC) Fingerprint Request Form
- The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
- The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eQIP).
- The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
- A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC), training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel

working under this contract must be maintained in the database of the Office of Personnel Management (OPM).

- The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
- Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
- Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

In accordance with VA Handbook 0710, Personnel Security and Suitability Program, the position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the PWS are:

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	☒	☐	☐
5.2	☐	☒	☐
5.3	☐	☒	☐
5.4	☐	☒	☐

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.

b. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the PAL template artifact. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no

longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

c. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.
d. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) Optional Form 306
    2) Self-Certification of Continuous Service
    3) VA Form 0710
    4) Completed SIC Fingerprint Request Form
e. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
f. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via e-QIP).
g. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
h. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed "Contractor Rules of Behavior", and with a valid, operational PIV credential for PIV-only logical access to VA's network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of OPM.
i. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
j. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
k. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies

and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:

A. Contractor Staff Roster

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: Markdown, MS Word 2010 or above, MS Excel 2010 or above, MS PowerPoint 2000 or above, MS Visio 2010 or above, and Adobe Postscript Data Format (PDF).

6.4 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Levels of Performance associated with this effort.

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Provides quality services/products	Satisfactory or higher
B. Project Milestones and Schedule	1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in accordance with the established schedule 3. Notifies customer in advance of potential problems	Satisfactory or higher
C. Cost & Staffing	1. Currency of expertise and staffing levels appropriate 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Management	1. Integration and coordination of all activities to execute effort	Satisfactory or higher
E. Deliverable Metric/SLA	Refer to individual Metric/SLA Specified in PWS Tasks	Refer to individual Metric/SLA Specified in PWS Tasks
F. User Experience	G. Usage data and analysis H. Customer satisfaction	

The COR will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable level of performance. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion.

6.4.1 DELIVERABLE METRICS/SERVICE LEVEL AGREEMENTS PERFORMANCE

The Contractor shall meet all SLAs as described in the PWS. However, if the Contractor's performance falls below a required service level, the Contractor shall only be paid for the lower service level provided. Please be advised that the VA's payment for the lower service level provided in no way waives the Government's right to pursue any remedies available by law, including, but not limited to, termination for breach of contract. Please be further advised that failure to meet the SLAs as set forth in this PWS shall be considered a condition endangering contract performance and may provide grounds for default termination. The Government will conduct a monthly review of the defined SLAs against the Contractor's performance/solution. If a lower service level is assessed in a particular month, the Contractor shall provide an itemized invoice detailing the lower service level price (percentage and amount) and deducting that lower service level price from the total monthly price of the applicable Contract Line Item Number in the following month's invoice. SLAs are set forth in PWS FFP tasks 5.2.2.

The Government will provide 100% of the FFP payment for API operations for every month that meets the SLAs for every metric (Service Availability, Service Reachability, Development Environment Availability).

The Government will provide 90% of the FFP payment for API operations for every month that does not meet the SLAs for every metric but does maintain availability and reachability above 99.0% for every metric.

The Government will provide 85% of the FFP payment for API operations for every month that does not meet the SLAs for every metric but does maintain availability and reachability between 98.0% and 99% for every metric.

The Government will provide 75% of the FFP payment for API operations for every month that does not meet the SLAs for every metric but does maintain availability and reachability between 95.0% and 98% for every metric.

The Government will not provide any FFP payment for API operations for any month that does not meet the SLAs for every metric and where availability and reachability are below 95.0% for every metric.

6.4.2 GOVERNMENT FURNISHED PROPERTY

The Government has determined that remote access solutions involving Citrix Access Gateway (CAG) have proven to be an unsatisfactory access method to complete the tasks on this specific contract The Government also understands that GFE is limited to Contractors requiring direct access to the network to: access development environments; install, configure and run TRM-approved software and tools; upload/download/ manipulate code, run scripts, apply patches, etc.; configure and change system settings; check logs, troubleshoot/debug, and test/QA.

Based on the Government assessment of remote access solutions and the requirements of this contract, the Government estimates that the following GFE may be required by this contract:

1. Standard laptops: Quantity to be determined based on team size and Quoters approach.

2. Developer-grade laptops: Quantity to be determined based on team size and Quoters approach.

The Government will not provide IT accessories including but not limited to Mobile Wi-Fi hotspots/wireless access points, additional or specialized keyboards or mice, laptop bags, extra charging cables, extra PIV readers, peripheral devices, additional RAM, etc. The Contractor is responsible for providing these types of IT accessories in support of the contract as necessary and any VA installation required for these IT accessories shall be coordinated with the COR.

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, unless the connection uses FIPS 140-2 (or its successor) validated encryption, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the PM, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

Each documented initiative under this contract incorporates VA Handbook 6500.6, "Contract Security," March 12, 2010 by reference as though fully set forth therein. The VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), and will be tracked therein. The TMS may be accessed at https://www.tms.va.gov. If you do not have a TMS profile, go to https://www.tms.va.gov and click on the "Create New User" link on the TMS to gain access.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance**.**

A2.1. VA Internet and Intranet Standards

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed and published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

A3.1. Section 508 – Electronic and Information Technology (EIT) Standards

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

- ☒ § 1194.21 Software applications and operating systems
- ☐ § 1194.22 Web-based intranet and internet information and applications
- ☐ § 1194.23 Telecommunications products
- ☐ § 1194.24 Video and multimedia products
- ☐ § 1194.25 Self-contained, closed products
- ☐ § 1194.26 Desktop and portable computers
- ☒ § 1194.31 Functional Performance Criteria
- ☒ § 1194.41 Information, Documentation, and Support

A3.2. Equivalent Facilitation

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, §1194.5. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

A3.3. Compatibility with Assistive Technology

The Section 508 standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device. Section 508 requires that the EIT be compatible with such software and devices so that EIT can be accessible to and usable by

individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

A3.4. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include final test results demonstrating Section 508 compliance.
Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government reserves the right to independently test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment.

Deliverables:

A. Final Section 508 Compliance Test Results

A4.0 Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

A5.0 Confidentiality and Non-Disclosure

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"). Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
    a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
    b. Controlled access to system and security software and documentation.
    c. Recording, monitoring, and control of passwords and privileges.
    d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
    e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.

f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
h. Contractor does not require access to classified data.

8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13693, "Planning for Federal Sustainability in the Next Decade", dated March 19, 2015; Executive Order 13221, "Energy-Efficient Standby Power Devices," dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

The Contractor shall ensure that information technology products are procured and/or services are performed with products that meet and/or exceed ENERGY STAR, FEMP designated, low standby power, and EPEAT guidelines. The Contractor shall provide/use products that earn the ENERGY STAR label and meet the ENERGY STAR specifications for energy efficiency. Specifically, the Contractor shall:

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).
2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements . The Contractor shall use the low standby power products specified at http://energy.gov/eere/femp/low-standby-power-products.

3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.

4. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.

The following is a list of information technology products for which ENERGY STAR, FEMP designated, low standby power, and EPEAT registered products are available:

1. Computer Desktops, Laptops, Notebooks, Displays, Monitors, Integrated Desktop Computers, Workstation Desktops, Thin Clients, Disk Drives
2. Imaging Equipment (Printers, Copiers, Multi-Function Devices, Scanners, Fax Machines, Digital Duplicators, Mailing Machines)
3. Televisions, Multimedia Projectors

This list is continually evolving, and as a result is not all-inclusive.

ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE

APPLICABLE PARAGRAPHS TAILORED FROM: *THE VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE, VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010*

B1. GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the CO immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The CO must also

be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic

storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

8. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

9. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA minimum requirements. VA Configuration Guidelines are available upon request.

10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA CO for response.

11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&A) or a Memorandum of Understanding-Interconnection Security Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, and the TIC Reference Architecture). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.*

2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 11 configured to operate on Windows 7 and future versions, as required.

3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default "program files" directory and silently install and uninstall.

4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

6. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

7. The Contractor/Subcontractor agrees to:

a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or

operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

i. The Systems of Records (SOR); and

ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

b. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

c. Include this Privacy Act clause, including this subparagraph (c), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR.

8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.

a. "Operation of a System of Records" means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

b. "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person's name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

c. "System of Records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or

known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical**,** but in no event longer than 5 days.

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes within 5 days.

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the CO and the VA Assistant Secretary for Office of Information and Technology.

B5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires A&A of the Contractor's systems in accordance with VA Handbook 6500.3, *Assessment, Authorization and Continuous Monitoring of VA Information Systems* and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection security agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA CO and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the A&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new A&A would be necessary.

e. The Contractor/Subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f.VA prohibits the installation and use of personally-owned or Contractor/Subcontractor owned equipment or software on the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software

must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

1) Vendor must accept the system without the drive;

2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;

a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

B6. SECURITY INCIDENT INVESTIGATION

a. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or

sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B7.LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract. However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.

b. The Contractor/Subcontractor shall provide notice to VA of a "security incident" as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that

incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

1) Nature of the event (loss, theft, unauthorized access);
2) Description of the event, including:
   a) date of occurrence;
   b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
3) Number of individuals affected or potentially affected;
4) Names of individuals or groups affected or potentially affected;
5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
6) Amount of time the data has been out of VA control;
7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
8) Known misuses of data containing sensitive personal information, if any;
9) Assessment of the potential harm to the affected individuals;
10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Breaches Involving Sensitive Personal Information*, as appropriate; and
11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1) Notification;
2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
3) Data breach analysis;
4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B8. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security

controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

B9. TRAINING

a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:
   1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Information Security Rules of Behavior, updated version located at https://www.voa.va.gov/DocumentView.aspx?DocumentID=4848, relating to access to VA information and information systems;
   2) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (TMS #10176) and complete this required privacy and information security training annually;
   3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access [to be defined by the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]

b. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 2 days of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

SECTION E - SOLICITATION PROVISIONS

E.1 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es):

http://www.acquisition.gov/far/index.html
http://www.va.gov/oal/library/vaar/

(End of Provision)

FAR Number	Title	Date
52.217-5	EVALUATION OF OPTIONS	JUL 1990

E.2 52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (JUL 2013)

(a) *Definitions.* As used in this provision—

"Administrative proceeding" means a non-judicial process that is adjudicatory in nature in order to make a determination of fault or liability (e.g., Securities and Exchange Commission Administrative Proceedings, Civilian Board of Contract Appeals Proceedings, and Armed Services Board of Contract Appeals Proceedings). This includes administrative proceedings at the Federal and State level but only in connection with performance of a Federal contract or grant. It does not include agency actions such as contract audits, site visits, corrective plans, or inspection of deliverables.

"Federal contracts and grants with total value greater than $10,000,000" means—

(1) The total value of all current, active contracts and grants, including all priced options; and

(2) The total value of all current, active orders including all priced options under indefinite-delivery, indefinite-quantity, 8(a), or requirements contracts (including task and delivery and multiple-award Schedules).

"Principal" means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a division or business segment; and similar positions).

(b) The offeror [ ] has [ ] does not have current active Federal contracts and grants with total value greater than $10,000,000.

(c) If the offeror checked "has" in paragraph (b) of this provision, the offeror represents, by submission of this offer, that the information it has entered in the Federal Awardee Performance and Integrity Information System (FAPIIS) is current, accurate, and complete as of the date of submission of this offer with regard to the following information:

(1) Whether the offeror, and/or any of its principals, has or has not, within the last five years, in connection with the award to or performance by the offeror of a Federal contract or grant, been the subject of a proceeding, at the Federal or State level that resulted in any of the following dispositions:

(i) In a criminal proceeding, a conviction.

(ii) In a civil proceeding, a finding of fault and liability that results in the payment of a monetary fine, penalty, reimbursement, restitution, or damages of $5,000 or more.

(iii) In an administrative proceeding, a finding of fault and liability that results in—

(A) The payment of a monetary fine or penalty of $5,000 or more; or

(B) The payment of a reimbursement, restitution, or damages in excess of $100,000.

(iv) In a criminal, civil, or administrative proceeding, a disposition of the matter by consent or compromise with an acknowledgment of fault by the Contractor if the proceeding could have led to any of the outcomes specified in paragraphs (c)(1)(i), (c)(1)(ii), or (c)(1)(iii) of this provision.

(2) If the offeror has been involved in the last five years in any of the occurrences listed in (c)(1) of this provision, whether the offeror has provided the requested information with regard to each occurrence.

(d) The offeror shall post the information in paragraphs (c)(1)(i) through (c)(1)(iv) of this provision in FAPIIS as required through maintaining an active registration in the System for Award Management database via https://www.acquisition.gov (see 52.204-7).

(End of Provision)

E.3 52.212-3 OFFEROR REPRESENTATIONS AND CERTIFICATIONS—COMMERCIAL ITEMS (NOV 2017)

The Offeror shall complete only paragraph (b) of this provision if the Offeror has completed the annual representations and certification electronically via the System for Award Management (SAM) Web site located at https://www.sam.gov/portal. If the Offeror has not completed the annual representations and certifications electronically, the Offeror shall complete only paragraphs (c) through (u) of this provision.

(a) *Definitions.* As used in this provision—

Economically disadvantaged women-owned small business (EDWOSB) concern means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States and who are economically disadvantaged in accordance with 13 CFR part 127. It automatically qualifies as a women-owned small business eligible under the WOSB Program.

Forced or indentured child labor means all work or service—

(1) Exacted from any person under the age of 18 under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily; or

(2) Performed by any person under the age of 18 pursuant to a contract the enforcement of which can be accomplished by process or penalties.

Highest-level owner means the entity that owns or controls an immediate owner of the offeror, or that owns or controls one or more entities that control an immediate owner of the offeror. No entity owns or exercises control of the highest level owner.

Immediate owner means an entity, other than the offeror, that has direct control of the offeror. Indicators of control include, but are not limited to, one or more of the following: Ownership or interlocking management, identity of interests among family members, shared facilities and equipment, and the common use of employees.

Inverted domestic corporation means a foreign incorporated entity that meets the definition of an inverted domestic corporation under 6 U.S.C. 395(b), applied in accordance with the rules and definitions of 6 U.S.C. 395(c).

Manufactured end product means any end product in product and service codes (PSCs) 1000-9999, except—

(1) PSC 5510, Lumber and Related Basic Wood Materials;
(2) Product or Service Group (PSG) 87, Agricultural Supplies;
(3) PSG 88, Live Animals;
(4) PSG 89, Subsistence;
(5) PSC 9410, Crude Grades of Plant Materials;
(6) PSC 9430, Miscellaneous Crude Animal Products, Inedible;
(7) PSC 9440, Miscellaneous Crude Agricultural and Forestry Products;
(8) PSC 9610, Ores;
(9) PSC 9620, Minerals, Natural and Synthetic; and
(10) PSC 9630, Additive Metal Materials.

Place of manufacture means the place where an end product is assembled out of components, or otherwise made or processed from raw materials into the finished product that is to be provided to the Government. If a product is disassembled and reassembled, the place of reassembly is not the place of manufacture.

Predecessor means an entity that is replaced by a successor and includes any predecessors of the predecessor.

Restricted business operations means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the business can demonstrate—

(1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;

(2) Are conducted pursuant to specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;

(3) Consist of providing goods or services to marginalized populations of Sudan;

(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;

(5) Consist of providing goods or services that are used only to promote health or education; or

(6) Have been voluntarily suspended.

"Sensitive technology"—

(1) Means hardware, software, telecommunications equipment, or any other technology that is to be used specifically—

(i) To restrict the free flow of unbiased information in Iran; or
(ii) To disrupt, monitor, or otherwise restrict speech of the people of Iran; and

(2) Does not include information or informational materials the export of which the President does not have the authority to regulate or prohibit pursuant to section 203(b)(3) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)).

Service-disabled veteran-owned small business concern—

(1) Means a small business concern—

(i) Not less than 51 percent of which is owned by one or more service-disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and

(ii) The management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a service-disabled veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran.

(2) Service-disabled veteran means a veteran, as defined in 38 U.S.C. 101(2), with a disability that is service-connected, as defined in 38 U.S.C. 101(16).

Small business concern means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR Part 121 and size standards in this solicitation.

Small disadvantaged business concern, consistent with 13 CFR 124.1002, means a small business concern under the size standard applicable to the acquisition, that—

(1) Is at least 51 percent unconditionally and directly owned (as defined at 13 CFR 124.105) by—

(i) One or more socially disadvantaged (as defined at 13 CFR 124.103) and economically disadvantaged (as defined at 13 CFR 124.104) individuals who are citizens of the United States; and

(ii) Each individual claiming economic disadvantage has a net worth not exceeding $750,000 after taking into account the applicable exclusions set forth at 13 CFR 124.104(c)(2); and

(2) The management and daily business operations of which are controlled (as defined at 13.CFR 124.106) by individuals, who meet the criteria in paragraphs (1)(i) and (ii) of this definition.

Subsidiary means an entity in which more than 50 percent of the entity is owned—

(1) Directly by a parent corporation; or

(2) Through another subsidiary of a parent corporation.

Successor means an entity that has replaced a predecessor by acquiring the assets and carrying out the affairs of the predecessor under a new name (often through acquisition or merger). The term "successor" does not include new offices/divisions of the same company or a company that only changes its name. The extent of the responsibility of the successor for the liabilities of the predecessor may vary, depending on State law and specific circumstances.

Veteran-owned small business concern means a small business concern—

(1) Not less than 51 percent of which is owned by one or more veterans (as defined at 38 U.S.C. 101(2)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and

(2) The management and daily business operations of which are controlled by one or more veterans.

Women-owned business concern means a concern which is at least 51 percent owned by one or more women; or in the case of any publicly owned business, at least 51 percent of its stock is owned by one or more women; and whose management and daily business operations are controlled by one or more women.

Women-owned small business concern means a small business concern—

(1) That is at least 51 percent owned by one or more women; or, in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and

(2) Whose management and daily business operations are controlled by one or more women.

Women-owned small business (WOSB) concern eligible under the WOSB Program (in accordance with 13 CFR part 127), means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States.

(b) (1) *Annual Representations and Certifications.* Any changes provided by the offeror in paragraph (b)(2) of this provision do not automatically change the representations and certifications posted on the SAM website.

(2) The offeror has completed the annual representations and certifications electronically via the SAM website access through http://www.acquisition.gov. After reviewing the SAM database information, the offeror verifies by submission of this offer that the representations and certifications currently posted electronically at FAR 52.212-3, Offeror Representations and Certifications—Commercial Items, have been entered or updated in the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer and are incorporated in this offer by reference (see FAR 4.1201), except for paragraphs .

(c) Offerors must complete the following representations when the resulting contract will be performed in the United States or its outlying areas. Check all that apply.

(1) *Small business concern*. The offeror represents as part of its offer that it [ ] is, [ ] is not a small business concern.

(2) *Veteran-owned small business concern.* [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.*] The offeror represents as part of its offer that it [ ] is, [ ] is not a veteran-owned small business concern.

(3) *Service-disabled veteran-owned small business concern.* [*Complete only if the offeror represented itself as a veteran-owned small business concern in paragraph (c)(2) of this provision.*] The offeror represents as part of its offer that it [ ] is, [ ] is not a service-disabled veteran-owned small business concern.

(4) *Small disadvantaged business concern.* [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.*] The offeror represents

that it [ ] is, [ ] is not a small disadvantaged business concern as defined in 13 CFR 124.1002.

(5) *Women-owned small business concern*. [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.*] The offeror represents that it [ ] is, [ ] is not a women-owned small business concern.

(6) WOSB concern eligible under the WOSB Program. [Complete only if the offeror represented itself as a women-owned small business concern in paragraph (c)(5) of this provision.] The offeror represents that—

(i) It [ ] is, [ ] is not a WOSB concern eligible under the WOSB Program, has provided all the required documents to the WOSB Repository, and no change in circumstances or adverse decisions have been issued that affects its eligibility; and

(ii) It [ ] is, [ ] is not a joint venture that complies with the requirements of 13 CFR part 127, and the representation in paragraph (c)(6)(i) of this provision is accurate for each WOSB concern eligible under the WOSB Program participating in the joint venture. [*The offeror shall enter the name or names of the WOSB concern eligible under the WOSB Program and other small businesses that are participating in the joint venture:* _____.] Each WOSB concern eligible under the WOSB Program participating in the joint venture shall submit a separate signed copy of the WOSB representation.

(7) Economically disadvantaged women-owned small business (EDWOSB) concern. [*Complete only if the offeror represented itself as a WOSB concern eligible under the WOSB Program in (c)(6) of this provision.*] The offeror represents that—

(i) It [ ] is, [ ] is not an EDWOSB concern, has provided all the required documents to the WOSB Repository, and no change in circumstances or adverse decisions have been issued that affects its eligibility; and

(ii) It [ ] is, [ ] is not a joint venture that complies with the requirements of 13 CFR part 127, and the representation in paragraph (c)(7)(i) of this provision is accurate for each EDWOSB concern participating in the joint venture. [*The offeror shall enter the name or names of the EDWOSB concern and other small businesses that are participating in the joint venture:* _____.] Each EDWOSB concern participating in the joint venture shall submit a separate signed copy of the EDWOSB representation.

Note: Complete paragraphs (c)(8) and (c)(9) only if this solicitation is expected to exceed the simplified acquisition threshold.

(8) *Women-owned business concern (other than small business concern).* [*Complete only if the offeror is a women-owned business concern and did not represent itself as a small business concern in paragraph (c)(1) of this provision.*] The offeror represents that it [ ] is a women-owned business concern.

(9) *Tie bid priority for labor surplus area concerns.* If this is an invitation for bid, small business offerors may identify the labor surplus areas in which costs to be incurred on account of manufacturing or production (by offeror or first-tier subcontractors) amount to more than 50 percent of the contract price: _____

(10) *HUBZone small business concern.* [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.*] The offeror represents, as part of its offer, that—

(i) It [ ] is, [ ] is not a HUBZone small business concern listed, on the date of this representation, on the List of Qualified HUBZone Small Business Concerns maintained by the Small Business Administration, and no material change in ownership and control, principal office, or HUBZone employee percentage has occurred since it was certified by the Small Business Administration in accordance with 13 CFR Part 126; and

(ii) It [ ] is, [ ] is not a joint venture that complies with the requirements of 13 CFR Part 126, and the representation in paragraph (c)(10)(i) of this provision is accurate for the HUBZone small business concern or concerns that are participating in the joint venture. [The offeror shall enter the name or names of the HUBZone small business concern or concerns that are participating in the joint venture:_____.] Each HUBZone small business concern participating in the joint venture shall submit a separate signed copy of the HUBZone representation.

(d) Representations required to implement provisions of Executive Order 11246—

(1) *Previous contracts and compliance*. The offeror represents that—

(i) It [ ] has, [ ] has not participated in a previous contract or subcontract subject to the Equal Opportunity clause of this solicitation; and

(ii) It [ ] has, [ ] has not filed all required compliance reports.

(2) *Affirmative Action Compliance.* The offeror represents that—

(i) It [ ] has developed and has on file, [ ] has not developed and does not have on file, at each establishment, affirmative action programs required by rules and regulations of the Secretary of Labor (41 CFR parts 60-1 and 60-2), or

(ii) It [ ] has not previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.

(e) *Certification Regarding Payments to Influence Federal Transactions* (31 U.S.C. 1352). (Applies only if the contract is expected to exceed $150,000.) By submission of its offer, the offeror certifies to the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress or an employee of a Member of Congress on his or her behalf in connection with

the award of any resultant contract. If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of the offeror with respect to this contract, the offeror shall complete and submit, with its offer, OMB Standard Form LLL, Disclosure of Lobbying Activities, to provide the name of the registrants. The offeror need not report regularly employed officers or employees of the offeror to whom payments of reasonable compensation were made.

(f) *Buy American Certificate*. (Applies only if the clause at Federal Acquisition Regulation (FAR) 52.225-1, Buy American—Supplies, is included in this solicitation.)

(1) The offeror certifies that each end product, except those listed in paragraph (f)(2) of this provision, is a domestic end product and that for other than COTS items, the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The offeror shall list as foreign end products those end products manufactured in the United States that do not qualify as domestic end products, i.e., an end product that is not a COTS item and does not meet the component test in paragraph (2) of the definition of "domestic end product." The terms "commercially available off-the-shelf (COTS) item," "component," "domestic end product," "end product," "foreign end product," and "United States" are defined in the clause of this solicitation entitled "Buy American—Supplies."

(2) Foreign End Products:

Line Item No	Country of Origin
_____	_____
_____	_____
_____	_____

[List as necessary]

(3) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25.

(g) (1) *Buy American—Free Trade Agreements—Israeli Trade Act Certificate.* (Applies only if the clause at FAR 52.225-3, Buy American—Free Trade Agreements—Israeli Trade Act, is included in this solicitation.)

(i) The offeror certifies that each end product, except those listed in paragraph (g)(1)(ii) or (g)(1)(iii) of this provision, is a domestic end product and that for other than COTS items, the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The terms "Bahrainian, Moroccan, Omani, Panamanian, or Peruvian end product," "commercially available off-the-shelf (COTS) item," "component," "domestic end product," "end product," "foreign end product," "Free Trade Agreement country," "Free Trade Agreement country end product," "Israeli end product," and "United States" are defined in the clause of this solicitation entitled "Buy American—Free Trade Agreements—Israeli Trade Act."

(ii) The offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled "Buy American—Free Trade Agreements—Israeli Trade Act":

Free Trade Agreement Country End Products (Other than Bahrainian, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:

Line Item No.	Country of Origin
_____	_____
_____	_____
_____	_____

[List as necessary]

(iii) The offeror shall list those supplies that are foreign end products (other than those listed in paragraph (g)(1)(ii) of this provision) as defined in the clause of this solicitation entitled "Buy American—Free Trade Agreements—Israeli Trade Act." The offeror shall list as other foreign end products those end products manufactured in the United States that do not qualify as domestic end products, i.e., an end product that is not a COTS item and does not meet the component test in paragraph (2) of the definition of "domestic end product."

Other Foreign End Products:

Line Item No.	Country of Origin
_____	_____
_____	_____
_____	_____

[List as necessary]

(iv) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25.

(2) *Buy American—Free Trade Agreements—Israeli Trade Act Certificate, Alternate I.* If Alternate I to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Canadian end products as defined in the clause of this solicitation entitled "Buy American—Free Trade Agreements—Israeli Trade Act":

Canadian End Products:

Line Item No.

_____
_____
_____

[List as necessary]

(3) *Buy American—Free Trade Agreements—Israeli Trade Act Certificate, Alternate II.* If Alternate II to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Canadian end products or Israeli end products as defined in the clause of this solicitation entitled "Buy American—Free Trade Agreements—Israeli Trade Act":

Canadian or Israeli End Products:

Line Item No.	Country of Origin
_____	_____
_____	_____
_____	_____

[List as necessary]

(4) *Buy American—Free Trade Agreements—Israeli Trade Act Certificate, Alternate III*. If Alternate III to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian, Korean, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled "Buy American—Free Trade Agreements—Israeli Trade Act":

Free Trade Agreement Country End Products (Other than Bahrainian, Korean, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:

Line Item No.	Country of Origin
_____	_____
_____	_____
_____	_____

[List as necessary]

(5) *Trade Agreements Certificate.* (Applies only if the clause at FAR 52.225-5, Trade Agreements, is included in this solicitation.)

(i) The offeror certifies that each end product, except those listed in paragraph (g)(5)(ii) of this provision, is a U.S.-made or designated country end product, as defined in the clause of this solicitation entitled "Trade Agreements".

(ii) The offeror shall list as other end products those end products that are not U.S.-made or designated country end products.

Other End Products:

Line Item No.	Country of Origin
_____	_____
_____	_____
_____	_____

[List as necessary]

(iii) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25. For line items covered by the WTO GPA, the Government will evaluate offers of U.S.-made or designated country end products without regard to the restrictions of the Buy American statute. The Government will consider for award only offers of U.S.-made or designated country end products unless the Contracting Officer determines that there are no offers for such products or that the offers for such products are insufficient to fulfill the requirements of the solicitation.

(h) *Certification Regarding Responsibility Matters* (Executive Order 12689). (Applies only if the contract value is expected to exceed the simplified acquisition threshold.) The offeror certifies, to the best of its knowledge and belief, that the offeror and/or any of its principals—

(1) [ ] Are, [ ] are not presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;

(2) [ ] Have, [ ] have not, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a Federal, state or local government contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or Commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property;

(3) [ ] Are, [ ] are not presently indicted for, or otherwise criminally or civilly charged by a Government entity with, commission of any of these offenses enumerated in paragraph (h)(2) of this clause; and

(4) [ ] Have, [ ] have not, within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds $3,500 for which the liability remains unsatisfied.

(i) Taxes are considered delinquent if both of the following criteria apply:

(A) *The tax liability is finally determined.* The liability is finally determined if it has been assessed. A liability is not finally determined if there is a pending administrative or judicial challenge. In the case of a judicial challenge to the

liability, the liability is not finally determined until all judicial appeal rights have been exhausted.

(B) *The taxpayer is delinquent in making payment.* A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection action is precluded.

(ii) *Examples.*

(A) The taxpayer has received a statutory notice of deficiency, under I.R.C. Sec. 6212, which entitles the taxpayer to seek Tax Court review of a proposed tax deficiency. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek Tax Court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(B) The IRS has filed a notice of Federal tax lien with respect to an assessed tax liability, and the taxpayer has been issued a notice under I.R.C. Sec. 6320 entitling the taxpayer to request a hearing with the IRS Office of Appeals contesting the lien filing, and to further appeal to the Tax Court if the IRS determines to sustain the lien filing. In the course of the hearing, the taxpayer is entitled to contest the underlying tax liability because the taxpayer has had no prior opportunity to contest the liability. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek tax court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(C) The taxpayer has entered into an installment agreement pursuant to I.R.C. Sec. 6159. The taxpayer is making timely payments and is in full compliance with the agreement terms. The taxpayer is not delinquent because the taxpayer is not currently required to make full payment.

(D) The taxpayer has filed for bankruptcy protection. The taxpayer is not delinquent because enforced collection action is stayed under 11 U.S.C. 362 (the Bankruptcy Code).

(i) *Certification Regarding Knowledge of Child Labor for Listed End Products (Executive Order 13126).*

(1) *Listed end products.*

Listed End Product	Listed Countries of Origin
_____	_____
_____	_____

(2) *Certification. [If the Contracting Officer has identified end products and countries of origin in paragraph (i)(1) of this provision, then the offeror must certify to either (i)(2)(i) or (i)(2)(ii) by checking the appropriate block.]*

[ ] (i) The offeror will not supply any end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product.

[ ] (ii) The offeror may supply an end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product. The offeror certifies that it has made a good faith effort to determine whether forced or indentured child labor was used to mine, produce, or manufacture any such end product furnished under this contract. On the basis of those efforts, the offeror certifies that it is not aware of any such use of child labor.

(j) *Place of manufacture.* (Does not apply unless the solicitation is predominantly for the acquisition of manufactured end products.) For statistical purposes only, the offeror shall indicate whether the place of manufacture of the end products it expects to provide in response to this solicitation is predominantly—

(1) __ In the United States (Check this box if the total anticipated price of offered end products manufactured in the United States exceeds the total anticipated price of offered end products manufactured outside the United States); or

(2) __ Outside the United States.

(k) *Certificates regarding exemptions from the application of the Service Contract Labor Standards.* (Certification by the offeror as to its compliance with respect to the contract also constitutes its certification as to compliance by its subcontractor if it subcontracts out the exempt services.)

[ ] (1) Maintenance, calibration, or repair of certain equipment as described in FAR 22.1003-4(c)(1). The offeror [ ] does [ ] does not certify that—

(i) The items of equipment to be serviced under this contract are used regularly for other than Governmental purposes and are sold or traded by the offeror (or subcontractor in the case of an exempt subcontract) in substantial quantities to the general public in the course of normal business operations;

(ii) The services will be furnished at prices which are, or are based on, established catalog or market prices (see FAR 22.1003- 4(c)(2)(ii)) for the maintenance, calibration, or repair of such equipment; and

(iii) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract will be the same as that used for these employees and equivalent employees servicing the same equipment of commercial customers.

[ ] (2) Certain services as described in FAR 22.1003- 4(d)(1). The offeror [ ] does [ ] does not certify that—

(i) The services under the contract are offered and sold regularly to non-Governmental customers, and are provided by the offeror (or subcontractor in the

case of an exempt subcontract) to the general public in substantial quantities in the course of normal business operations;

(ii) The contract services will be furnished at prices that are, or are based on, established catalog or market prices (see FAR 22.1003-4(d)(2)(iii));

(iii) Each service employee who will perform the services under the contract will spend only a small portion of his or her time (a monthly average of less than 20 percent of the available hours on an annualized basis, or less than 20 percent of available hours during the contract period if the contract period is less than a month) servicing the Government contract; and

(iv) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract is the same as that used for these employees and equivalent employees servicing commercial customers.

(3) If paragraph (k)(1) or (k)(2) of this clause applies—

(i) If the offeror does not certify to the conditions in paragraph (k)(1) or (k)(2) and the Contracting Officer did not attach a Service Contract Labor Standards wage determination to the solicitation, the offeror shall notify the Contracting Officer as soon as possible; and

(ii) The Contracting Officer may not make an award to the offeror if the offeror fails to execute the certification in paragraph (k)(1) or (k)(2) of this clause or to contact the Contracting Officer as required in paragraph (k)(3)(i) of this clause.

(l) *Taxpayer Identification Number (TIN)* (26 U.S.C. 6109, 31 U.S.C. 7701). (Not applicable if the offeror is required to provide this information to the SAM database to be eligible for award.)

(1) All offerors must submit the information required in paragraphs (l)(3) through (l)(5) of this provision to comply with debt collection requirements of 31 U.S.C. 7701(c) and 3325(d), reporting requirements of 26 U.S.C. 6041, 6041A, and 6050M, and implementing regulations issued by the Internal Revenue Service (IRS).

(2) The TIN may be used by the Government to collect and report on any delinquent amounts arising out of the offeror's relationship with the Government (31 U.S.C. 7701(c)(3)). If the resulting contract is subject to the payment reporting requirements described in FAR 4.904, the TIN provided hereunder may be matched with IRS records to verify the accuracy of the offeror's TIN.

(3) *Taxpayer Identification Number (TIN).*

[ ] TIN: _____.
[ ] TIN has been applied for.
[ ] TIN is not required because:
[ ] Offeror is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the United

States and does not have an office or place of business or a fiscal paying agent in the United States;
[ ] Offeror is an agency or instrumentality of a foreign government;
[ ] Offeror is an agency or instrumentality of the Federal Government.

(4) *Type of organization.*

[ ] Sole proprietorship;
[ ] Partnership;
[ ] Corporate entity (not tax-exempt);
[ ] Corporate entity (tax-exempt);
[ ] Government entity (Federal, State, or local);
[ ] Foreign government;
[ ] International organization per 26 CFR 1.6049-4;
[ ] Other _____.

(5) *Common parent.*

[ ] Offeror is not owned or controlled by a common parent;
[ ] Name and TIN of common parent:
Name _____.
TIN _____.

(m) *Restricted business operations in Sudan.* By submission of its offer, the offeror certifies that the offeror does not conduct any restricted business operations in Sudan.

(n) *Prohibition on Contracting with Inverted Domestic Corporations*.

(1) Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with either an inverted domestic corporation, or a subsidiary of an inverted domestic corporation, unless the exception at 9.108-2(b) applies or the requirement is waived in accordance with the procedures at 9.108-4.

(2) *Representation*. The Offeror represents that—

(i) It [ ] is, [ ] is not an inverted domestic corporation; and

(ii) It [ ] is, [ ] is not a subsidiary of an inverted domestic corporation.

(o) *Prohibition on contracting with entities engaging in certain activities or transactions relating to Iran.*

(1) The offeror shall email questions concerning sensitive technology to the Department of State at CISADA106@state.gov.

(2) *Representation and certifications.* Unless a waiver is granted or an exception applies as provided in paragraph (o)(3) of this provision, by submission of its offer, the offeror—

(i) Represents, to the best of its knowledge and belief, that the offeror does not export any sensitive technology to the government of Iran or any entities or individuals owned or controlled by, or acting on behalf or at the direction of, the government of Iran;

(ii) Certifies that the offeror, or any person owned or controlled by the offeror, does not engage in any activities for which sanctions may be imposed under section 5 of the Iran Sanctions Act; and

(iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds $3,500 with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (see OFAC's Specially Designated Nationals and Blocked Persons List at *http://www.treasury.gov/ofac/downloads/t11sdn.pdf*).

(3) The representation and certification requirements of paragraph (o)(2) of this provision do not apply if—

(i) This solicitation includes a trade agreements certification (*e.g.,* 52.212–3(g) or a comparable agency provision); and

(ii) The offeror has certified that all the offered products to be supplied are designated country end products.

(p) *Ownership or Control of Offeror*. (Applies in all solicitations when there is a requirement to be registered in SAM or a requirement to have a unique entity identifier in the solicitation).

(1) The Offeror represents that it [ ] has or [ ] does not have an immediate owner. If the Offeror has more than one immediate owner (such as a joint venture), then the Offeror shall respond to paragraph (2) and if applicable, paragraph (3) of this provision for each participant in the joint venture.

(2) If the Offeror indicates "has" in paragraph (p)(1) of this provision, enter the following information:

Immediate owner CAGE code: ____.
Immediate owner legal name: ____.
(*Do not use a "doing business as" name*)
Is the immediate owner owned or controlled by another entity: [ ] Yes or [ ] No.

(3) If the Offeror indicates "yes" in paragraph (p)(2) of this provision, indicating that the immediate owner is owned or controlled by another entity, then enter the following information:

Highest-level owner CAGE code: ____.
Highest-level owner legal name: ____.
(*Do not use a "doing business as" name*)

(q) *Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law.*

(1) As required by sections 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts, The Government will not enter into a contract with any corporation that—

(i) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or

(ii) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(2) The Offeror represents that—

(i) It is [ ] is not [ ] a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and

(ii) It is [ ] is not [ ] a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(r) *Predecessor of Offeror*. (Applies in all solicitations that include the provision at 52.204-16, Commercial and Government Entity Code Reporting.)

(1) The Offeror represents that it [ ] is or [ ] is not a successor to a predecessor that held a Federal contract or grant within the last three years.

(2) If the Offeror has indicated "is" in paragraph (r)(1) of this provision, enter the following information for all predecessors that held a Federal contract or grant within the last three years (if more than one predecessor, list in reverse chronological order):

Predecessor CAGE code: ____ (or mark "Unknown").
Predecessor legal name: ____.
(Do not use a "doing business as" name).

(s) [Reserved]

(t) *Public Disclosure of Greenhouse Gas Emissions and Reduction Goals*. Applies in all solicitations that require offerors to register in SAM (52.212-1(k)).

(1) This representation shall be completed if the Offeror received $7.5 million or more in contract awards in the prior Federal fiscal year. The representation is optional if the Offeror received less than $7.5 million in Federal contract awards in the prior Federal fiscal year.

(2) Representation. [Offeror to check applicable block(s) in paragraph (t)(2)(i) and (ii)]. (i) The Offeror (itself or through its immediate owner or highest-level owner) [ ] does, [ ] does not publicly disclose greenhouse gas emissions, i.e., makes available on a publicly accessible Web site the results of a greenhouse gas inventory, performed in accordance with an accounting standard with publicly available and consistently applied criteria, such as the Greenhouse Gas Protocol Corporate Standard.

(ii) The Offeror (itself or through its immediate owner or highest-level owner) [ ] does, [ ] does not publicly disclose a quantitative greenhouse gas emissions reduction goal, i.e., make available on a publicly accessible Web site a target to reduce absolute emissions or emissions intensity by a specific quantity or percentage.

(iii) A publicly accessible Web site includes the Offeror's own Web site or a recognized, third-party greenhouse gas emissions reporting program.

(3) If the Offeror checked "does" in paragraphs (t)(2)(i) or (t)(2)(ii) of this provision, respectively, the Offeror shall provide the publicly accessible Web site(s) where greenhouse gas emissions and/or reduction goals are reported:_____.

(u) (1) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions), Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with an entity that requires employees or subcontractors of such entity seeking to report waste, fraud, or abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(2) The prohibition in paragraph (u)(1) of this provision does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(3) Representation. By submission of its offer, the Offeror represents that it will not require its employees or subcontractors to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the performance of a Government contract to a designated investigative or law enforcement representative

of a Federal department or agency authorized to receive such information (e.g., agency Office of the Inspector General).

(End of Provision)

E.4 52.216-1 TYPE OF CONTRACT (APR 1984)

The Government contemplates award of a hybrid firm-fixed-price (FFP) and Time and Materials/Labor Hour Task Order resulting from this solicitation.

(End of Provision)

E.5 52.227-15 REPRESENTATION OF LIMITED RIGHTS DATA AND RESTRICTED COMPUTER SOFTWARE (DEC 2007)

(a) This solicitation sets forth the Government's known delivery requirements for data as defined in the clause at 52.227-14, Rights in Data—General. Any resulting contract may also provide the Government the option to order additional data under the Additional Data Requirements clause at 52.227-16, if included in the contract. Any data delivered under the resulting contract will be subject to the Rights in Data—General clause at 52.227-14 included in this contract. Under the latter clause, a Contractor may withhold from delivery data that qualify as limited rights data or restricted computer software, and deliver form, fit, and function data instead. The latter clause also may be used with its Alternates II and/or III to obtain delivery of limited rights data or restricted computer software, marked with limited rights or restricted rights notices, as appropriate. In addition, use of Alternate V with this latter clause provides the Government the right to inspect such data at the Contractor's facility.

(b) By completing the remainder of this paragraph, the offeror represents that it has reviewed the requirements for the delivery of technical data or computer software and states [offeror check appropriate block]—

[ ] (1) None of the data proposed for fulfilling the data delivery requirements qualifies as limited rights data or restricted computer software; or

[ ] (2) Data proposed for fulfilling the data delivery requirements qualify as limited rights data or restricted computer software and are identified as follows:

_____

_____

(c) Any identification of limited rights data or restricted computer software in the offeror's response is not determinative of the status of the data should a contract be awarded to the offeror.

(End of provision)

E.6 52.233-2 SERVICE OF PROTEST (SEP 2006)

(a) Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from:

Hand-Carried Address:

Department of Veterans Affairs
Technology Acquisition Center
23 Christopher Way
Eatontown, NJ 07724

Mailing Address:

Department of Veterans Affairs
Technology Acquisition Center
23 Christopher Way
Eatontown, NJ 07724

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

(End of Provision)

E.7 VAAR 852.233-70 PROTEST CONTENT/ALTERNATIVE DISPUTE RESOLUTION (JAN 2008)

(a) Any protest filed by an interested party shall:

(1) Include the name, address, fax number, and telephone number of the protester;
(2) Identify the solicitation and/or contract number;
(3) Include an original signed by the protester or the protester's representative and at least one copy;
(4) Set forth a detailed statement of the legal and factual grounds of the protest, including a description of resulting prejudice to the protester, and provide copies of relevant documents;
(5) Specifically request a ruling of the individual upon whom the protest is served;
(6) State the form of relief requested; and
(7) Provide all information establishing the timeliness of the protest.

(b) Failure to comply with the above may result in dismissal of the protest without further consideration.

(c) Bidders/offerors and contracting officers are encouraged to use alternative dispute resolution (ADR) procedures to resolve protests at any stage in the protest process. If ADR is used, the Department of Veterans Affairs will not furnish any documentation in an ADR proceeding beyond what is allowed by the Federal Acquisition Regulation.

(End of Provision)

E.8 VAAR 852.233-71 ALTERNATE PROTEST PROCEDURE (JAN 1998)

As an alternative to filing a protest with the contracting officer, an interested party may file a protest with the Deputy Assistant Secretary for Acquisition and Materiel Management, Acquisition Administration Team, Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420, or for solicitations issued by the Office of Construction and Facilities Management, the Director, Office of Construction and Facilities Management, 810 Vermont Avenue, NW., Washington, DC 20420. The protest will not be considered if the interested party has a protest on the same or similar issues pending with the contracting officer.

PLEASE NOTE: The correct mailing information for filing alternate protests is as follows:

Deputy Assistant Secretary for Acquisition and Logistics,
Risk Management Team, Department of Veterans Affairs
810 Vermont Avenue, N.W.
Washington, DC 20420

Or for solicitations issued by the Office of Construction and Facilities Management:

Director, Office of Construction and Facilities Management
811 Vermont Avenue, N.W.
Washington, DC 20420

(End of Provision)

E.9 BASIS FOR AWARD

Comparative evaluation will be performed in accordance with Federal Acquisition Regulation (FAR) 13.106-2(b)(3). The Government will award a contract from this Request for Quote (RFQ) to the responsible Quoter whose quote conforms to the requirements of the RFQ and represents the best overall value to the Government with appropriate consideration given to the following evaluation Factors: Technical and Price. The Technical Factor is significantly more important than the Price Factor. The Government reserves the right to select a response that provides benefit to the Government that exceeds the minimum requirement. The Government is not requesting or accepting alternate quotes. The Government reserves the right to award to a Quoter with other than the lowest price. The Government reserves the right to award to multiple Quoters.

All quotes shall be subject to evaluation by a team of Government personnel. The Government intends to make an award selection without clarifications and/or discussions, but may determine after evaluating the quotes submitted that clarifications and/or discussions are necessary and conduct them as appropriate. The quote will be evaluated strictly in accordance with its written content.

The Government will conduct a comparative evaluation of Quoter’s responses based upon the following criteria:

1. TECHNICAL: The Government will evaluate the documentation on a previously developed and operated RESTful API in a production system and the written response, as required at RFQ Section E.10(i)(1) and (2), to determine the Quoter's capability and suitability to build and operate APIs as required in the Performance Work Statement (PWS). The documentation on a previously developed RESTful API in a production system will be evaluated based on API documentation best practices, such as, but not limited to: being machine readable; giving enough information for a developer to effectively use the API; and having realistic and complete request and response examples.

   Additionally, the quote will be evaluated to determine the extent to which it clearly demonstrates meeting and/or exceeding the technical elements identified in the submission instructions at RFQ Section E.10(i)(3).

   Finally, the response will be evaluated based on adherence to agile methodology and practices found within the Digital Services Playbook (https://playbook.cio.gov/).

2. PRICE: The Government will evaluate the price by adding the total of all line item prices, including all optional tasks. The Total Evaluated Price will be that sum.

E.10 QUOTE SUBMISSION INSTRUCTIONS

The Quote shall be submitted electronically by the date and time indicated in the RFQ via the Virtual Office of Acquisition (VOA) in the files set forth below by the date and time indicated in the RFQ. Quotes submitted by any other method will not be. File sizes shall not exceed 100MB. The web address for the VOA site is https://www.voa.va.gov/. Quoters will be required to be registered users on the VOA website to submit quotes. Once registered, Quoters can click on the Proposal Dashboard link and within that link click on Add Proposal to open up the form to upload files. The Proposal Type drop down field should be changed to 36C10B18Q3124 to reflect the RFQ being proposed against. Please see Section D, Attachment 003 – VOA Proposal Dashboard Instructions and Attachment 004 – VOA User Registration for additional information concerning VOA use and registration. For registration or technical issues concerning proposal submission, contact voahelp@va.gov.

Quoter's responses shall be submitted in accordance with the following instructions:

1) All pages are numbered, including attachments,
2) All documents are formatted to 8 ½ x 11 paper, and;
3) All documents are single-spaced, 12-point Times New Roman font, with a minimum of 1-inch margins;
4) A Cover Page, Table of Contents and/or a glossary of abbreviations or acronyms will not be included in the page counts identified below of the Quote. However, be advised that any and all information contained within any Table of Contents and/or glossary of abbreviations or acronyms submitted with the quote will not be evaluated by the Government. Responses to Price, RFQ, Quote, and Award Documents and Certifications/Representations will not be included in the page count of the Quote.

Late quotes will not be accepted for evaluation. To avoid submission of late quotes, we recommend the transmission of your proposal file 24 hours prior to the required proposal

due date and time. Please be advised that timeliness is determined by the date and time an Quoter's proposal is received by the Government not when an Quoter attempted transmission. Quoters are encouraged to review and ensure that sufficient bandwidth is available on their end of the transmission.

(i) TECHNICAL:

1. The Quoter shall provide API documentation on a previously developed RESTful API in a production system. (No Page Limitation). If the API documentation exists at a public URL, a link to that URL (in addition to the requirements in the next paragraph to verify when it was created) is sufficient. If the documentation is provided as a file or multiple files with the proposal, Quoter may submit up to 1 page of instructions as a README file for how it suggests the Government should review the documentation to receive maximum value from it. An example would be if documentation is delivered as a YAML file that meets the OpenAPI Specification and Quoter suggests the Government copies the contents of the file into https://editor.swagger.io to view the documentation most effectively (rather than reading the YAML directly).

   To ensure the documentation delivered is actually and entirely from a previously developed API and not created or altered for this RFQ, Quoters shall provide either a URL, such as to GitHub or other version control system, where the version control history and timestamps can be verified (ideal) or a point of contact for the client the API documentation was delivered to who can verify this is the same API documentation received at any point prior to August 20, 2018. The API documentation on a previously developed RESTful API in a production system must have been developed by your company or any proposed subcontractor who will be responsible for at least 40% of your proposed approach.

2. The Quoter shall provide a written response (limited to 7 pages) describing the how the API was built and operated, specifically addressing the following:
   - Why was the API created?
   - Who you worked with to build the API and when and how you worked with them?
   - How you decided upon scope for a Minimum Viable Product (MVP), how you validated the MVP met users' needs, and if/how you iterated beyond the MVP?
   - How was the API deployed to various environments?
   - Key Performance Indicators (KPIs) that were created for the API and how those were evaluated and met?
   - How you worked with partner systems or other API, system, or data integrations?
   - The process by which new customers could begin using the API and how the team engaged with potential and existing customers?

3. The Quoter shall provide a written response (limited to 10 pages) describing the following.

a. The Quoter shall describe its approach to developing and operating APIs in accordance with PWS task 5.2 and its subtasks including the proposed technology stack. The Quoter shall describe how it will organize sprint teams and the composition of each sprint team.

b. The Quoter shall describe its approach to developing and operating the API Gateway in accordance with PWS Task 5.3 and its subtasks including its proposed architecture, functionality, and technology stack for the API Gateway.

(ii) PRICE FACTOR: The Quoter shall complete the VA API Development and Operations Excel Price Evaluation Spreadsheet, found as Attachment 005 in the RFQ. The Total Evaluated Price shall be based on the information provided in the Excel Price Evaluation Spreadsheet. The Section B.4 Price Schedule of the RFQ is for informational purposes only and shall not be completed.

The Government anticipates that the number of sprints and the total price of CLIN 0002 in conjunction with the total prices of CLINs 0003, 0006 and 0007 should maximize the Governments budget and Subpart 13.5 – Simplified Procedures for Certain Commercial Items threshold of $7M.

The Quoter shall propose the unit price per sprint and complete the quantity of sprints it can accomplish in a 12-month period for the total price proposed for CLIN 0002.

The estimated labor hours identified in VA API Development and Operations Excel Price Evaluation Spreadsheet, found as Attachment 005 of the RFQ are for evaluation purposes only and do not obligate the Government to award such labor hours. The Quoter shall provide blended loaded labor rates (a single loaded labor rate for the prime contractor and all subcontractors) for each labor category. The Quoter shall use the labor categories set forth in the VA API Development and Operations Excel Price Evaluation Spreadsheet, with the qualifications and experience as described in Section D, Attachment 002. To the extent necessary, equivalent labor categories may be proposed by Quoters; however, explanations as to how such proposed labor categories meet and/or exceed the provided labor categories shall be provided and evaluated as part of the Quoter's technical response.

Price Rounding Issue - The Government requires Quoters to propose unit prices and total prices that are two decimal places and requires the unit prices and total prices to be displayed as two decimal places. Ensure that the two-digit unit price multiplied by the item quantity equals the two-digit total item price (there should be no rounding).

All Quoters should propose using an estimated award date of September 30, 2018.

(iiiv) **SOLICITATION, QUOTE, AND AWARD DOCUMENTS AND CERTIFICATIONS/REPRESENTATIONS:**

Certifications and Representations - An authorized official of the firm shall sign the SF 1449 and all certifications requiring original signature. An Acrobat PDF file shall be created to capture the signatures for submission. This submission shall contain the following:

(1) RFQ Section A – Standard Form (SF1449) and Acknowledgement of Amendments, if any.

(2) Any proposed terms and conditions and/or assumptions upon which the proposal is predicated. The Quoter is hereby advised that any Quoter-imposed terms and conditions and/or assumptions which deviate from the Government's material terms and conditions established by the RFQ, may result in delays of contract award.

(3) Representation that the Quoter has reviewed Section E.9 of the RFQ, and clause 52.227-15, and completed the appropriate certification in subparagraph (b) concerning the requirements for the delivery of technical data or computer software."